Balancing Privacy Rights & Innovation: Analysing the Digital Personal Data Protection Act, 2023 in the Context of AI Advancements

SHORT SYNOPSIS

Submitted in partial fulfilment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

to

Manav Rachna University

by

Laalima Gupta

Reg. No. -MRULWDN012K210021

Under the supervision of

Dr Tarundeep Kaur

Associate Professor, Department of Law

Dr Seema Gupta (Co-Supervisor)

Associate Professor (Adjunct), Department of Law

Department of Law
School of Law

MANAV RACHNA vidyanatariksha
MANAV RACHNA UNIVERSITY
Declared as State Private University vide Haryana Act 26 of 2014

MANAV RACHNA UNIVERSITY

Year 2025

MANAV RACHNA UNIVERSITY

Declared as State Private University vide Haryana Act 26 of 2014

MANAV RACHNA UNIVERSITY

Date: 5-12-2025

DECLARATION BY THE SCHOLAR

I hereby declare that the short synopsis "**Balancing Privacy Rights & Innovation: Analysing the Digital Personal Data Protection Act, 2023 in the Context of AI Advancements**" being submitted in the partial fulfilment of the requirement for the degree of Doctor of Philosophy in the department of Law under the School of Law of Manav Rachna University, Faridabad during the academic year 2025-26.

It is a bonafide record of original work carried out under the supervision of **Dr Tarundeep Kaur and Dr. Seema Gupta** and has not been submitted in full or part to any other university or institute for a degree or diploma. Further, it is certified that the short synopsis is within the plagiarism limit and a copy of the same is attached as per University norms.

Laalima Gupta

Reg. No. -MRULWDN012K210021

MANAV RACHNA UNIVERSITY

Declared as State Private University vide Haryana Act 26 of 2014

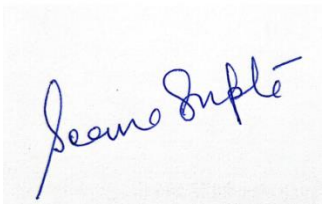
MANAV RACHNA UNIVERSITY

Date: 5-12-2025

CERTIFICATE BY SUPERVISOR(S)

This is to certify that, the short synopsis entitled **"Balancing Privacy Rights & Innovation: Analysing the Digital Personal Data Protection Act, 2023 in the Context of AI Advancements"** is an original piece of work done by research scholar **Laalima Gupta** under the supervision of **Dr. Tarundeep Kaur** and co-supervision of **Dr. Seema Gupta** for the degree of Doctor of Philosophy in the **Department of Law** under the **School of Law** of Manav Rachna University, Faridabad during the academic year **2025-26.**

Further, it is certified that the short synopsis is within the plagiarism limit and copy of the same is attached as per the University norms.



Supervisor

Dr. Tarundeep Kaur,
Associate Professor,
School of Law, MRU

Co-Supervisor

Dr. Seema Gupta
Associate Professor (Adjunct)
School of Law, MRU

ABSTRACT

Imagine this, it is a normal Monday morning, an individual unlocks their phone, and just like that their entire day is quietly choreographed by Artificial Intelligence (AI). The navigation application on the phone suggests a better route to the office, that saves them from traffic and saves fuel. A credit card application pops open a notification confirming the pre-approval of a loan based on the digital footprints that it had gathered over a period of several months. The CCTV cameras across the bustling city, analyze the flow of the crowd to improve safety. In educational institutions, the new adaptive learning platforms adjust the syllabus based on the learners' capabilities. Today, none of the above instances feels futuristic anymore.

Why?

Because somehow, AI has become an ordinary part of our lives. In a world where AI is advancing at the speed of light, what remains unseen is the plethora of Personal Data that aid these conveniences to become a real-life possibility, and the unfathomable power that moves to the those who collect this data, process it, and then potentially infer from it.

The proficiencies of AI, like recognizing patterns, predicting behaviors, and conclusively shaping the decisions of the user, keeps on snowballing with every new AI model. Although, these capabilities better expediencies, productivity, inclusions, and public services, it also exposed its users to profiling, discrimination, and loss of autonomy when data is collected without a clear consent, pooled beyond their original purpose, and retained for an unnecessarily longer time.

Today, it is beyond imagination as to how easy it is to re-identify, anonymized data. Redressal is difficult for the ones that have been affected by the opaqueness of the automated decision-making. What makes AI useful in these times, also has the power to make consent fragile, because the signs of the same are too dense, choices are binary, and the withdrawal often comes with friction, it is rarely smooth. This tension between innovation and privacy is no longer abstract policy debate. It is a lived reality for citizens, entrepreneurs, and regulators.

In such an out of equilibrium digital landscape, India has introduced its Digital Personal Data Protection Act, 2023, which serves as a principal legal safeguard. The Act clearly defines the rights and duties based relationship between the users, termed as the “Data Principal” and the “Data Fiduciary”, the entity that determines the purpose and the means of the data processing.

This study aims to investigate the actual impact of AI on the “Privacy and Freedom of Expression” of individual citizens with a view to assessing the current position of AI laws and the future requirements of AI Laws in India. The requirement of AI has become inescapable today to meet the routine requirements of the ever-burgeoning human enterprise. Computer machines today display AI and are capable of processing, deciphering, inferring, identifying patterns from the plethora of available user data feeds and predicting decisions and outcomes, even surpassing human intelligence. The ever-increasing use of AI technologies by public, private and corporate enterprises, on one hand, immensely benefits the general public at large, but, on the other hand, puts their “privacy and freedom of expression” at risk. The question arises, why then, the AI laws and governance all over the world including India, seem to be in wait-and-watch mode? Do the benefits from AI far outnumber the risks?

Keywords: AI, Privacy, Freedom of Speech, Pervasive, AI Laws

TABLE OF CONTENTS

S.no	Description	Page No.
1.	**Introduction** 1.1 Power of AI in the Data-Driven World 1.2 All Pervasive Nature of AI 1.3 Laws on Protection of Human Rights: Privacy and Freedom 1.4 Present Landscape of AI Laws 1.5 Why the World Goes Slow on AI Laws 1.6 AI a Necessity: Gathering Momentum 1.7 The Devil of all Pervasive and Intrusive AI	**1-4**
2.	**Literature Review**	**5-8**
3.	**Description of Broad Area**	**9-10**
4.	**Research Questions**	**11**
5.	**Objectives of the Study**	**12**
6.	**Hypothesis**	**13**
7.	**Methodology to be adopted**	**14**
8.	**Expected Outcome of the Research**	**15**
9.	**Tentative Chapterization**	**16**
10.	**Bibliography**	**17**

1. INTRODUCTION

1.1 Power of AI in the Data-Driven World

In 2006 Clive Robert Humby a British mathematician and entrepreneur in the field of Data Science coined the phrase "**Data is the new oil**". Michael Palmer expanded on Humby's quote by saying "**Like oil data is valuable but if unrefined it cannot be really used**". Data is indeed the most valuable commodity today and it is being refined not only at a fantastic pace but in fantastic ways as well. Computer machines today, display **AI** and are capable of processing, deciphering, inferring, identifying patterns from the available personal user data uploaded on the virtual world, and predicting decisions and outcomes, to surpass human intelligence.[1]

1.2 AI and its All-Pervasive Characteristic

AI today has not only become pervasive but has also become invasive and intrusive in our personal, professional, and social lives. The ever-increasing use of AI technologies by public, private and corporate enterprises, on one hand, immensely benefits the public at large, but, on the other hand, puts their privacy and freedom of expression at risk.[2]

Search Engines churn out multiple suggestions based on our internet surfing proclivity. Our media feeds are being curated and integrated consumer devices monitor our digital activity through smart chatbot online assistants, filters for spam removal, autocorrect and autofill intrusions. Traffic movements, electrical transformer grids and stations and supplies of water in an area, are now being regulated using AI technologies. Autonomous vehicles and remote control of home utilities devices are becoming a norm. Organisations are employing biometrics i.e., fingerprints, facial cues and IRIS for surveillance and monitoring. People using smartphones have their medical history, shopping preferences, political inclination, religious orientation, financial transactions, food, literature, and entertainment preferences all

[1] Shrestha, Y. R., Ben-Menahem, S. M., & von Krogh, G. (2019). Organizational Decision-Making Structures in the Age of Artificial Intelligence. California Management Review, 61(4), 66–83.
[2] Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. Philosophy & Technology, 35(1).

being monitored, recorded, deciphered, inferred, and processed for profiling & pattern determination to predict our choices, decisions, and actions. While mankind is aware of some of these things happening, a lot happens without their knowledge, which threatens their privacy and freedom of expression.[3]

1.3 Privacy Related Laws under the Umbrella of Human Rights Laws

Article 12 and Article 19 of the Universal Declaration of Human Rights (UDHR)[4], recognise the right to privacy, respectively, as fundamental human rights.

Article 17 of the International Covenant on Civil and Political Rights (ICCPR)[5] recognises the right to privacy as a fundamental human right.

Article 21, of the Constitution of India, provides for the right to life which includes privacy. The right to privacy is a pre-requisite to freedom of expression and without these rights citizens of the world will not be able to express themselves freely.[6]

While there are international and national laws that guarantee the right to privacy there is a need to study the adequacy of specific AI laws in the context of privacy and freedom of expression. Before looking at the Indian policy framework of AI laws it would be worthwhile to study the landscape of international, regional, and national laws about AI around the world.

1.4AI Laws and their present global framework and landscape

In the global landscape, apart from the European unions, elaborate GDPR, there is no substantial piece of paper that specifically addresses the privacy concerns of users digitally. This European Regulation is also limited to the European continent and seizes to apply beyond its boundaries. At national level, several nations have attempted to address the debate between innovation, AI advancement and privacy, but nothing concrete has been established till date. All one can refer to, are case laws, directions, observations of the Courts, etc. The

[3] Bernal, P., 2018. Data privacy beyond the human. International Review of Law, Computers & Technology, 32(1), pp. 65-80.
[4] United Nations. (1948). *Universal Declaration of Human Rights*.https://www.un.org/en/about-us/universal-declaration-of-human-rights
[5] United Nations (General Assembly), 1966, art. 17
[6] Gupta, A., 2021. AI and the right to privacy in India: Legal challenges and prospects. Indian Journal of Cyber Law and Security, 5(2), pp. 41-64.

only Law specific to AI, being developed at present along with the DPDPA, 2023 is the 'EU AI Act'.[7]

It, therefore, becomes apparent that the world has gone slow in legislating and enacting AI-specific laws in general and AI-specific laws that would guarantee the right to privacy and freedom of expression. The countries, rather than legislating and enacting rigid laws, are following a flexible approach by issuing guidelines, codes of ethics and advisories to technological business organisations, that design, produce, implement and exploit AI technologies. The approach promotes self-regulation and self-audit in the production and application of AI technologies.

India too, has adopted a self-regulating and self-audit approach and like the rest of the world, currently, there are no specific laws in India, regulating AI. The Ministry of Electronics and Information Technology (MEITY) has constituted four committees to develop a policy framework for regulating AI. The over-arching thought that rules the minds of Indian policymakers is that the existing laws in India are sufficient to tackle the challenges of AI and require only some sector-specific modifications and alignments.[8] The existing policy document on AI suggests seven broad guiding principles to be followed as a part of self-regulation i.e., safety & reliability, equality, inclusivity & non-discrimination, transparency, accountability, and protection & reinforcement of positive human values.[9]

1.5 Why the World Goes Slow on AI-Laws?

will highlight as to why the nations of the world and India are deliberately going slow on AI-specific laws, even as the risks to the privacy of digital users are growing day by day with the exponential growth of AI. The research will also bring out the fact that mankind, today, has already crossed a '**Point of no Return'** with regard to our dependence on AI and its inevitable growth in future. In the last 50 years, the world population has more than doubled

[7] The European Union's Artificial Intelligence Act, 2021 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

[8] Artificial intelligence committees' reports | Ministry of Electronics and Information Technology, Government of India. (n.d.). Ministry of Electronics and Information Technology, Government of India |. https://www.meity.gov.in/artificial-intelligence-committees-reports

[9] (n.d.). NITI Aayog. https://www.niti.gov.in/sites/default/files/2023-03/Responsible-AI-AIForAll-Approach-Document-for-India-Part-Principles-for-Responsible-AI.pdf

from 3.8 billion to approximately 8 billion today. [10]Indian population has almost trebled in the same period from 55 crores to 140 crores today. To support this human explosion and the consequent human enterprise, human intelligence is too slow and inadequate to sustain mankind. We require machines to process, glean, recognize patterns, infer and predict our intent, behaviour, and decisions and to do much more in future.

1.6 AI a Necessity: Gathering Momentum

On 22 March 2023, the Prime Minister of India unveiled a vision document for 6G which will further enable and exploit AI. On 18 March 2023, an AI bot-enabled surrogate journalist 'SANA' interacted with the PM at the India Today Conclave.

The world wants AI to surpass human capabilities which is already the case and feel comforted when machines remember data as it saves time.[11] Humans have become used to, rather feeling comforted when a machine gathers, identifies patterns and predicts their intent and are delighted with their instant visibility on digital media, as they readily volunteer their personal data.[12]

1.7 The Devil of all Pervasive and Intrusive AI

At the same time, there is a sense of insecurity as some people feel harassed when agencies retain their data and exploit it against their wishes.[13] Their expression is stifled when they find out their online activities or what they have posted online has now been automatically moderated, filtered, or removed. There is a feeling of exposure when individuals are picked up in a crowd by a facial recognition AI tool. When agencies know and predict patterns of thinking, choices, and decisions that humans are likely to make, places they visited, places they are likely to visit in future, what they spoke and what they could speak, it makes them feel insecure, harassed, and infringed with respect of the privacy rights.

---

[10] https://www.cnbctv18.com. (2022, November 15). Day of 8 billion: How the global population has doubled in 50 years and now what? cnbctv18.com. https://www.cnbctv18.com/world/day-of-8-billion-global-world-population-doubled-in-50-years-15165041.htm

[11] Desai, N., 2020. AI, free speech, and the Indian Constitution. Indian Constitutional Law Review, 9(3), pp. 29-53.

[12] Borgesius, F.J.Z., and Koops, B.J., 2019. AI and the right to privacy. European Data Protection Law Review, 5(2), pp. 115-131.

[13] Khanna, P., 2022. AI and the right to privacy in India: A comparative study with GDPR. European Journal of Law and Technology, 13(1), pp. 22-45.

2. LITERATURE REVIEW

The debate between privacy rights and innovation over the years has changed. Earlier it was "whether to use the data," but with the fast-changing times, the contemporary debate has shifted to "how to use the data" without converting humans into eternally predictable and legible profiles.[14] If we come to think of it, initially privacy in broad parlance meant "the right to be left alone",[15] but later, with the digitalization, it came to be understood as the "right of an individual" over their personal information.[16] As per the classic scholarship on modern privacy and Solove's taxonomy, it is evident that privacy harms includes a bundle of harms such as exposure, exclusion, surveillance, secondary use, aggregation, etc., and is no just limited to "someone finding out about a secret" anymore.[17]

However, the digital infrastructures have given a reality check to the idea of privacy, since realistically privacy cannot be "managed" by individuals anymore simply through noticing and making a choice about it, it's more complicated, as collection of personal data is now a continuous and opaque process bundles into everyday necessities.[18] This complexity has pushed the scholarship on privacy to much better and richer accounts; it is now an institutional and social condition that protects the equality, autonomy, and the democratic participation of an individual, and not merely secrets.[19]

One of the central propositions of this research is that "privacy harms" are often contextual; meaning, the same set of data can be appropriate in one context, and inappropriate or unjust in another. Under the "contextual integrity" theory as explained by Nissenbaum, privacy norms are described as flowing of improper information that run counter to context-specific norms about 'who shares the information? 'with whom that information is shared?' 'what kind of information?' and 'under which transmission principles?'[20]

---

[14] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.
[15] Ibid
[16] Alan F. Westin, *Privacy and Freedom* (Antheneum 1967).
[17] Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880.
[18] Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477. *Available at:*https://scholarship.law.gwu.edu/context/faculty_publications/article/2074/viewcontent/A_Taxonomy_of_Privacy.pdf (Visited on Feb. 22, 2025)
[19] Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).
[20] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 *Washington Law Review* 119.

This theoretical framework is crucially relevant for all systems developed for the AI, that re-route data across contexts, for example; a health query becomes an ad signal; a retail chat becomes training data; a workplace tool becomes behavioral scoring.[21] Similarly, the data economy, elucidates how the personalization and prediction markets have incentivized on the extraction of user data, beyond the user's reasonable expectations, thereby creating "structural pressures" to push such business models in surveillance-oriented directions.[22] Scholars have described this as "surveillance capitalism"[23] or even "data colonialism," where human experience is appropriated as raw material for economic value and control.[24]

There are 3-ways in which the privacy risks get intensified due AI driven technologies; firstly, they enable *inferencing*, meaning, systems are now capable of inferring to ostensibly mundane data and then generating highly sensitive attributes, turning the non-sensitive inputs into high-stakes judgements, for example, the purchase histories, browsing patterns, purchase histories, etc.[25] Secondly, AI facilitates *scalability* and *persistence*, allowing models to systematically reuse data over stretched periods and among numerous users, which complicates the practical purpose of data usage and retention.[26]

And thirdly, AI creates new avenues for leakage of data; training data can be unintentionally exposed through model responses or malicious attacks, and sensitive personal characteristics can be recreated or identified using methods like membership inference and model inversion.[27] Research on large AI models indicates that data memorization and extraction are not merely theoretical concerns, particularly when these models are trained on vast datasets and subsequently subjected to adversarial queries.[28]

---

[21] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2009).
[22] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019).
[23] Ibid.
[24] Nick Couldry and Ulises A Mejias, 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject' (2019) 20(4) *Television & New Media* 336.
[25] Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' (2016) 54(2) *Journal of Economic Literature* 442.
[26] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (John Murray 2013).
[27] Reza Shokri and others, 'Membership Inference Attacks Against Machine Learning Models' (2017) *IEEE Symposium on Security and Privacy* 3.
[28] Nicholas Carlini and others, 'Extracting Training Data from Large Language Models' (2021) *USENIX Security Symposium.*

The legal design does not differ from this technical literature much, instead it unswervingly informs that how user rights like 'erasure of data,' 'consent withdrawal,' and 'purposeful limitation of data,', can credibly be implemented by the 'learning' objects, even after the 'raw records of data' have been deleted.[29]

The concepts of 'selective forgetting' and 'machine unlearning' have therefore become relevant to the theory of Data Protection, since it recontextualizes erasure from a mere database transaction to a comprehensive lifecycle governance issue involving training sets, checkpoints, derived embeddings, and deployed copies.[30]

Parallelly, it is argued by legal scholarship that 'consent' often fails as an effective protector when it comes to digital personal data as the user undergoes an overload of cognitive experiences, information asymmetry, and comes across tons of take-it-or-leave-it platforms.[31] The choice architecture that surrounds the user in the virtual world, can be manipulative even when consent was formally obtained in the first place. This renders the whole concept of consent substantively weak, even though its procedurally valid.[32]

This poses a dominant challenge for the analysis of the DPDPA, 2023, considering the fact that law relies on notice and consent heavily, and that AI systems basically flourish and grow on secondary use, aggregation, and repurposing of user data.

A second line of critical evaluation focuses on distributional harms i.e., AI systems can amplify discrimination by translating "historical bias" into "automated rules", while retaining opacity and denying affected users' practical recourse.[33]

The fairness literature and its socio-legal critical evaluation emphasizes that privacy is intertwined with equality and non-discrimination. Profiling and ranking often concentrate harm on marginalized groups, even when the system never "intends" discrimination.[34] This intersects

[29] Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 4.5.2016.
[30] Antigoni Tzitzika Bourtoule and others, 'Machine Unlearning' (2021) *IEEE Symposium on Security and Privacy*.
[31] Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880.
[32] Deceptive design/dark patterns literature; see generally Arunesh Mathur and others, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' (2019) *Proceedings of the ACM on Human-Computer Interaction* 1.
[33] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown 2016).
[34] Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 *California Law Review* 671.

with the concept of “group privacy” and “collective harms”, where injury arises not only from individual identification, but from statistical treatment of categories and communities.[35]

A significant corpus of work has focused on automated decision-making and the related drive for procedural protections-transparency, explanation, and the right to contest decisions.[36] In EU data protection discourse, Article 22 of the GDPR[37], read along with other related provisions, generated debate about whether there is a "right to explanation" at all, and what kind of explanation would be legally and practically meaningful?[38] Many scholars warn that thin explanations are in danger of amounting to little more than "transparency theatre" unless accompanied by auditability, accountability, and accessible redress.[39]

In response to these constraints, proposals for technical governance have emerged, including documentation practices, such as datasheets for datasets, model cards, impact assessments, and external audits.[40] These frame transparency as an ecology of evidence rather than a singular disclosure.

[35] A Taylor, L Floridi and B van der Sloot (eds*), Group Privacy: New Challenges of Data Technologies* (Springer 2017).
[36] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).
[37] Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119 4.5.2016, art 22 (‘Automated individual decision-making, including profiling’)
[38] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, ‘Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation’ (2017) 7(2) *International Data Privacy Law* 76.
[39] Joshua A Kroll and others, ‘Accountable Algorithms’ (2017) 165 *University of Pennsylvania Law Review* 633.
[40] Timnit Gebru and others, ‘Datasheets for Datasets’ (2018) arXiv:1803.09010; Margaret Mitchell and others, ‘Model Cards for Model Reporting’ (2019) *Proceedings of FAT** 220.

3. DESCRIPTION OF BROAD AREA

- **The Scope and Realm of Research**

Technology not only transcends boundaries but also the mediums and spaces known to mankind. The stretch of technology extends from tangibility to intangibility. AI not only aids and supplements Human Intelligence but in future will replace Human Intelligence completely

Understanding the Difference Between Human and AI

In order to frame laws on AI to safeguard Privacy and Freedom of Expression we need to understand the basic difference between "Human Intelligence" and "Artificial Intelligence". We must know how the human brain works and what are its limitations which AI overcomes easily. There is a need to understand as to how the Human Mind remembers and forgets information. How human mental processes differ from AI in remembering and forgetting data.

- **Understanding the Pervasive Nature of AI**

The study would bring out how AI has become pervasive in our daily lives. How algorithmic and automated decision making has replaced human decision making. How mankind is becoming irreversibly dependent on AI. The study brings out the inevitability of the eventual replacement of Human Intelligence by AI. In multiple ways, only AI, going ahead in future will be able to support mankind and its burgeoning enterprise.

- **Estimating the Future of AI to set a framework for AI Laws**

The research will delve in-depth into the growth of Generative AI leading to AI Singularity in future. This would give us an idea of the type of AI laws that would last the exponential growth of AI and still remain relevant. A brief look at the exponential possibilities in the future development of AI would be required.

Identifying the Stakeholders and the Interested Parties

The study would bring out how governments, corporations, technology companies and the general public at large are rushing to enhance their AI status and qualifications. The interested

parties would definitely be the AI developers and the technology companies. A brief look at the exponential possibilities in the future development of AI.

- **AI Laws and Governance**

The study would bring out the adverse impact of AI on Privacy and Freedom of Expression and bring out the present landscape of AI Laws and Governance. A study of the Adequacy of Present Laws will be made. The study would bring out the dilemma which governments face in implementing AI Laws in the context of Privacy and Freedom of Expression and bring out the need to find the solution to the dilemma in implementing AI Laws.

4. RESEARCH QUESTIONS

Q1. Whether DPDPA 2023 addresses adequately the problems and challenges of AI today, like that of profiling of users and automated decision-making?

Q2. Are there going to be potential clashes between privacy rights of users under the DPDPA 2023 provisions and the advancement of AI and innovation?

Q3. What are the difference between the DPDPA, 2023 and the GDPR?

Q4. Whether the enforcement strategies of the DPDP Act, 2023, are effective so as to regulating AI technology's use of data?

Q5. Whether any changes could be suggested for DPDP Act, 2023, to find a better middle ground between AI advancements and protection of privacy?

5. OBJECTIVES OF THE STUDY

- To Assess the Impact of AI on Privacy and Freedom of Expression
- To Examine Legal and Ethical Frameworks? Of what?
- To Identify Emerging Trends and Challenges
- To Propose Policy and Legal Recommendations
- To Contribute to Academic Discourse

6. HYPOTHESIS

A. India's DPDPA 2023 may not fully address AI-specific issues like automated decision-making because enhancing protections could include requiring clear consent and providing more detailed explanations to individuals.
B. Potential conflicts between AI advancement and privacy regulations under India's DPDPA are expected in large-scale data analytics, indicating a need for clearer AI-specific guidelines and increased transparency.
C. The effectiveness of the DPDP Act in regulating AI might be limited due to difficulties in monitoring AI compliance, suggesting a need for more specialised enforcement tools and greater regulatory expertise.

7. RESEARCH METHODOLOGY

The research will adopt a doctrinal research methodology, which primarily involves a comprehensive analysis of the relevant laws, regulations, policies, and case laws. This methodology will enable a systematic investigation of the legal aspects of AI and its impact on freedom of expression and the right to privacy in India.

A. Data Collection

Primary Sources: Constitutional provisions, judicial decisions, statutes and regulations.

Secondary Sources:

a. Academic Literature: Review of scholarly articles, books, and research papers discussing AI, freedom of expression, and the right to privacy in India and globally.

b. Reports and Policy Documents: Analysis of government and non-government reports and policy documents related to AI and its implications on human rights.

c. International Law: Examination of international legal instruments and guidelines on AI and human rights to gain a broader perspective.

B. Data Analysis

Comparative Analysis: Comparison of the Indian legal framework on AI with the international best practices and guidelines to identify potential gaps and areas of improvement.

Critical Analysis: Evaluation of the adequacy of the current AI laws and regulations in India in safeguarding the rights to freedom of expression and privacy.

8. EXPECTED OUTCOME OF RESEARCH

Today we are dealing with 'Artificial Narrow Intelligence' and are not more than a decade away from the concept of 'AI Singularity'. As AI today progresses toward AI Singularity, there have to be some reliable and acceptable guarantees to preserve our right to privacy and freedom of expression.[41] The requirement is to have some evergreen AI-specific laws which are legislated without the fear of scuttling the growth of AI on which mankind has become irreversibly dependable.

closely study the nature and characteristics of AI, especially in terms of, how machines '*remember and forget data'*. To ensure the right to privacy and freedom of expression humans would require machines to *forget* their personal data when they want.

The study would carry out an in-depth analysis of the present Indian approach to the framing of AI Laws, which includes concepts like *Differential Privacy, Federated Learning, Pre-hoc and Post-hoc techniques, zero-knowledge protocols, homomorphic encryption* and encouraging technology developers in self-regulation and self-audit on the same lines as IBM's *'AI Fairness 360'* and Google's *'What If'* tools.

The study would test the hypothesis that the growth of AI is inevitable, the dependence, especially in the context of India, on AI is irreversible and to preserve the right to privacy and freedom of expression there is a need for innovative AI Laws and collaborative approach that meets the requirements of AI technology stake-holders and also guarantees the right to privacy and freedom of expression at the same time.

[41] Cohen, J. (2019). Turning Privacy Inside Out. *Theoretical Inquiries in Law*, *20*(1), 1-31. https://doi.org/10.1515/til-2019-0002

9. TENTATIVE CHAPTERS

- Introduction: The concept of Artificial Intelligence and the Privacy Rights
- The evolution of AI and regulating AI advancement and Usage
- Global Data Protection Frameworks (GDPR) and the DPDP Act: Comparative Insights
- Adequacy of DPDP Act in Balancing Innovation and Individual Rights
- Judicial Trends in Balancing AI's Advancements & Privacy Rights
- Conclusion and Recommendations: Navigating A Way Forward

10. BIBLIOGRAPHY

Bansal, S., 2018. The role of AI in transforming the legal landscape in India. Indian Journal of Law and Technology, 14(1), pp. 1-29.

Bernal, P., 2018. Data privacy beyond the human. International Review of Law, Computers & Technology, 32(1), pp. 65-80.

Borgesius, F.J.Z., and Koops, B.J., 2019. AI and the right to privacy. European Data Protection Law Review, 5(2), pp. 115-131.

Desai, N., 2020. AI, free speech, and the Indian Constitution. Indian Constitutional Law Review, 9(3), pp. 29-53.

Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. Philosophy & Technology, 35(1).

Gupta, A., 2021. AI and the right to privacy in India: Legal challenges and prospects. Indian Journal of Cyber Law and Security, 5(2), pp. 41-64.

Khanna, P., 2022. AI and the right to privacy in India: A comparative study with GDPR. European Journal of Law and Technology, 13(1), pp. 22-45.

Shrestha, Y. R., Ben-Menahem, S. M., & von Krogh, G. (2019). Organizational Decision-Making Structures in the Age of Artificial Intelligence. California Management Review, 61(4), 66–

MANAV RACHNA UNIVERSITY

Swami Vivekananda Library and Resource Centre
Manav Rachna University

SIMILARITY VERIFICATION CERTIFICATE

Title: BALANCING PRIVACY RIGHTS & INNOVATION: ANALYSING THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023, IN CONTEXT OF AI ADVANCEMENT

Researcher: LAALIMA GUPTA

Registration Number: MRULWDN012K0021

Supervisor: DR. TARUNDEEP KAUR

Department: LAW

This is to certify that the above mentioned Short Synopsis/Thesis was scanned for similarity index through DRILLBIT Software on 5-12-25 with submission ID 4811140 and the similarity index was found to be 3 %. The complete report running into 19 Pages, 4789 Word count with File Size 196 KB is being forwarded to the Research Supervisor/DRC/DRB for review.

Date: 5-12-25

The complete report of the above Short Synopsis/Thesis has been reviewed and the similarity index is below the accepted norms as per the University Grants Commission (Promotion of Academic Integrity and Prevention of Plagiarism in Higher Educational Institutions) Regulations 2018. The Short Synopsis/Thesis may be considered for further processing

Laalima 5/12/25
Research Scholar

Seema Gupta
Research Supervisor
DR TARUNDEEP KAUR (SUP
DR SEEMA GUPTA (CO-SUP

DrillBit

Excluding matches
less than 14 words

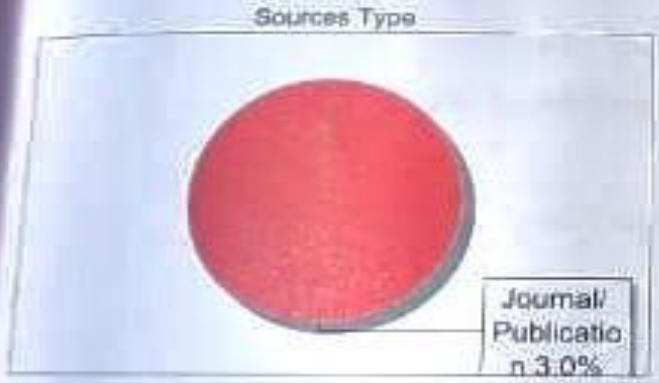
The Report is Generated by DrillBit Plagiarism Detection Software

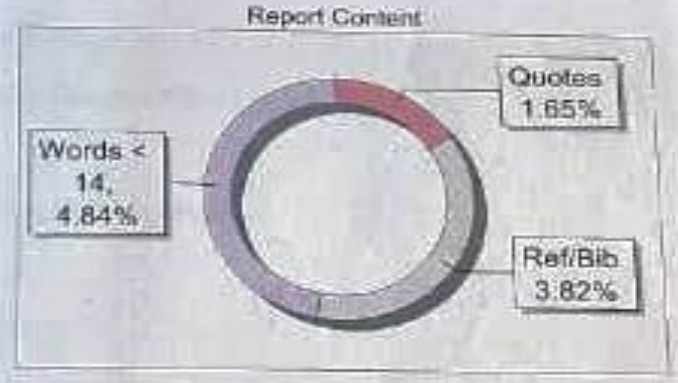
Submission Information

Author Name	Laalima Gupta
Title	Balancing Privacy Rights & Innovation: Analysing the Digital Personal Data Protection Act, 2023 in the Context of AI
Paper/Submission ID	4811140
Submitted by	netrapal.library@mru.edu.in
Submission Date	2025-12-05 12:18:43
Total Pages, Total Words	19, 4789
Document type	Synopsis

Result Information

Similarity 3 %





Exclude Information

Quotes	Excluded
References/Bibliography	Excluded
Source: Excluded < 14 Words	Excluded
Excluded Source	0 %
Excluded Phrases	Not Excluded

Database Selection

Language	English
Student Papers	Yes
Journals & publishers	Yes
Internet or Web	Yes
Institution Repository	Yes

A Unique QR Code use to View/ Download/ Share Pdf File

DrillBit

Excluding matches less than 14 words

Similarity Report

3	4	A	A-Satisfactory (0-10%) B-Upgrade (11-40%) C-Poor (41-60%) D-Unacceptable (61-100%)
SIMILARITY %	MATCHED SOURCES	GRADE	

MATCHED DOMAIN	%	SOURCE TYPE
ssl.ac.in	1	Publication
arxiv.org	1	Publication
ijirl.com	<1	Publication
ijirl.com	<1	Publication

Balancing Privacy Rights & Innovation: Analysing the Digital Personal Data Protection Act, 2023 in the Context of AI Advancements

SHORT SYNOPSIS

by

Laalima Gupta

Registration number:

Under the supervision of

Dr Tarundeep Kaur (Supervisor)

&

Dr Seema Gupta (Co-Supervisor)

Year 2025

MANAV RACHNA UNIVERSITY

ABSTRACT

Imagine this, it is a normal Monday morning, an individual unlocks their phone, and just like that their entire day is quietly choreographed by Artificial Intelligence (AI). The navigation application on the phone suggests a better route to the office, that saves them from traffic and saves fuel. A credit card application pops open a notification confirming the pre-approval of a